Today's Ransomware – Nemty Special Edition

May. 6, 2020

1. Blocked by trueEP®

? TrojanCut Ent 2. 0			- 🗆 ×
å [≥]			
्र एप हम		날짜 프로세스 •06 11:20:03 이력서_200506(파일이름 Behavior Blocking
🎧 스마트 백업			
김사 제외			
	■ 백업 로그	<u>찾기</u> 1000개 더 파일이름	복원 삭제
ତ୍ତେ ପ୍ରାଣାଣ			
දිටු			
⑦ 도움말			

2. Victim in case trueEP[®] was not installed - All file name's extensions were changed to NEMTY_random.

🔒 🛃 📙 🗸 새 쫄더				- 🗆	×
파일 홈 공유	보기				~ ?
← → · ↑ 🗛 → 새	폴더	~ 0	시 폴더 검색		Q
💻 Ч РС 🔷	이름	수정한 날짜	유형	크기	
🧊 3D 개체	NEMTY_83AY3XP-DECRYPT.txt	2020-05-06 오전	텍스트 문서	ЗКВ	
🖊 다운로드	📄 문서1.docx.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	17KB	
🚆 동영상	📄 문서2.docx.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	17KB	
🔮 문서	📄 문서3.docx.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	17KB	
- 바탕 화면	📄 문서4.xlsx.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	18KB	
■ 사진	📄 문서5.pptx.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	5,527KB	
	🗋 문서6.pdf.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	128KB	
♪ 음악	🗋 문서7.txt.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	2KB	
🏪 로컬 디스크 (C	📄 압축.zip.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	3,488KB	
👸 CD 드라이브 (🗋 압축2.zip.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	7,687KB	
🐂 라이브러리	📄 이미지.bmp.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	159KB	
🔿 네트워크	이미지.JPG.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	283KB	
🔤 제어판	📄 이미지.png.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	23KB	
🔊 휴지통	📄 이미지.psd.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	397KB	
	📄 이미지2.jpg.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	195KB	
▲새 폴더 🗸	📄 이미지3.jpg.NEMTY_83AY3XP	2020-05-06 오전	NEMTY_83AY3X	198KB	
16개 항목					

3. Screen of Victim

//// NEMTY_83AY3XP-DECRYPT.txt - Windows 메모장				—		×
파일(F) 편집(E) 서식(O) 보기(V) 도움말						
NEMTY SPECIAL EDITION						\wedge
We are sorry to inform but your files we Don't try to find free solution You will or We use strong encryption (AES-128-CTR 8	nly waste your time	9!				
Contacts:						
e-mail(main): spaxl425@protonmail.com e-mail(reserve): spaxl425@aol.com						
KEY: vh5vj1pr95JojRRuxNZOEpWthHrLmF9iiAxPY bBBP/HLtHuphW0qLL6xjdHXgSkDllwnoUUP 2oHeSmK24OuaVz2wOX6M7Pj0ODzyy6J3Tz	PQz0CP3gZp7zp+uG	G8kWRX	XclzMlcwm7B+p	pgublk	K+HrLF	FWI
٢	Ln 1, Col 1	100%	Windows (CRLF)	UTF-	2	>
	LITT, COLT	10078	Windows (CREF)	Uns	3	
휴지통 문서7.txt.N Microsoft Find NEMTY_83	Dear test rry Your files were o BAY3XP-DECRYPT.txt ry SPECIAL EDITIO	t and ma				







새 폴더



ii <mark>e </mark> 💼 💼

4. The results of Virus Total

	4001043072302107108722	dc17afadde150ea03e2be99e5	36C4D			Q	Q	<u>^</u>	Sign
22	() 22 engines detec	ted this file							C 2
Community Score		1725021e7f0a722dc17afadde150e 면 최선을 다해서 열심히 하겠습니다				020-05-06 02: moment ago	24:20 UTC	>	EXE
DETECTION	DETAILS BEHAV	IOR COMMUNITY							
Acronis	(1) Suspic	ious		SecureAge APEX	(1) Malicio	115			
BitDefenderTheta		N.ZexaF.34108.nq0@aKk1yAl		CrowdStrike Falcon		licious_confic	lence 100	% (D)	
Cybereason	() Maliclo			Cylance	() Unsafe				
eGambit	-	AI_Score_92%		Endgame		us (high Confi	idence)		
FireEye	-	c.mg.8bdfb96004038094		Fortinet		yptik.HDCUlt			
Ikarus		Win32.Tofsee		K7GW		ol (70000786			
Kaspersky	-	langerousObject.Multi.Generic		Microsoft		n:Win32/Gen			
Rising		re.Heuristic!ET#85% (RDMK:cmR	t	Sangfor Engine Zero	() Malwar				
SentinelOne (Static I	-	Suspicious PE		Sophos ML	 Heurist 				
Symantec		' ribute.HighConfidence		Trapmine		ous.low.ml.sc	ore		
VBA32	() BScop	e. Trojan. Zbot. 01439		ZoneAlarm by Check I	Point () UDS:D	angerousObje	ect.Multi.Ge	eneric	
Ad-Aware	⊘ Undete			AegisLab	Undete				
AhnLab-V3	⊘ Undete	ected		Alibaba	Undete	cted			
ALYac	⊘ Undete	ected		Antiy-AVL	 Undete 	cted			
Arcabit	O Undete	ected		Avast	 Undete 	cted			
Avast-Mobile	O Undete	ected		AVG	 Undete 	cted			
Avira (no cloud)	O Undete	ected		Baidu	 Undete 	cted			
BitDefender	Undete	ected		Bkav	 Undete 	cted			
CAT-QuickHeal	O Undete	ected		ClamAV	⊘ Undete	cted			
СМС	⊘ Undete	ected		Comodo	Undete	cted			
Cyren	⊘ Undete	acted		DrWeb	Undete	cted			
Emsisoft	O Undete	acted		eScan	Undete	cted			
ESET-NOD32	⊘ Undete	ected		F-Prot	 Undete 	cted			
F-Secure	⊘ Undete	ected		GData	Undete	cted			
Jiangmin	⊘ Undete	ected		K7AntiVirus	 Undete 	cted			
Kingsoft	⊘ Undete	ected		Malwarebytes	 Undete 	cted			
MAX	⊘ Undete	ected		MaxSecure	 Undete 	cted			
McAfee	⊘ Undete	ected		McAfee-GW-Edition	 Undete 	cted			
NANO-Antivirus	⊘ Undete	ected		Palo Alto Networks	 Undete 	cted			
Panda	⊘ Undete	ected		Qihoo-360	Undete	cted			
Sophos AV	⊘ Undete	ected		SUPERAntiSpyware	⊘ Undete	cted			
TACHYON	⊘ Undete	ected		Tencent	⊘ Undete	cted			
TrendMicro	⊘ Undete	ected		TrendMicro-HouseCal	I 🕢 Undete	cted			
VIPRE	⊘ Undete	ected		ViRobot	Undete	cted			
Webroot	⊘ Undete	acted		Yandex	✓ Undete	cted			
Zillya	⊘ Undete	ected		Zoner	⊘ Undete	cted			
Symantec Mobile Ins	sight 📎 Unable	to process file type		Trustlook					
VirusTot		Community	Tools		Premium Services		Docume		
Contact I How It Wo Terms of S Privacy Po Blog	orks Service	Join Community Vote and Comment Contributors Top Users Latest Comments	API Scripts YARA Desktop Apps Browser Exten Mobile App	sions	Intelligence Hunting Graph API v3 v2 Monitor		Get Starte Searching Reports API v3 v Use Case	2	G